Attorney's Docket No. 032326-025

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
Gilles Lisimaque	Group Art Unit: 2135
Application No.: 09/576,412	Examiner: Beemnet Dada
Filed: May 22, 2000	Appeal No.:
For: PROCESS TO MANAGE DATA IN A CHIP CARD	

APPEAL BRIEF

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This appeal is from the decision of the Primary Examiner dated January 27, 2005 finally rejecting claims 1-17, which are reproduced as the Claims Appendix of this brief.

☒ A check covering the ☐ $250.00 (2402) ☒ $500.00 (1402) Government fee is filed herewith.

☐ Charge ☐ $250.00 (2402) ☐ $500.00 (1402) to Credit Card. Form PTO-2038 is attached.

The Commissioner is hereby authorized to charge any appropriate fees under 37 C.F.R. §§1.16, 1.17, and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800.

Table of Contents

I. Real Party in Interest

The subject application, and the invention to which it is directed, are assigned to Gemplus, a French corporation.

II. Related Appeals and Interferences

There are no known appeals, interferences or judicial proceedings which may be related to, directly affect or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. Status of Claims

The application contains claims 1-17, all of which are pending and stand finally rejected. All pending claims are being appealed.

IV. Status of Amendments

There were no Amendments filed subsequent to the final Office Action.

V. Summary of Claimed Subject Matter

The claimed invention is directed to the management of data stored in a smart card, and is particularly concerned with the transfer of data from one card to another, such as in the case where the original card is about to expire and be replaced by a new card. (Page 1, lines 7-11). As is conventional, a smart card provides secure access to the data stored on the card, by requiring a user to enter a secret code, such as a PIN. This code is compared with a code stored in the memory of the smart card, which is referred to in the application as a management code. (Page 2, lines 1-7). The claimed invention provides a method for generating a management code for the new card that is based upon information relating to the old card. (Page 2, lines 19-22)

Referring to an embodiment illustrated in Figure 2 of the application, the management code 14 for the first card 9 is generated by an algorithm 13, based upon a mother key 100 and the serial number 12 of the first card. (Page 5, lines 6-12). This serial number is also stored on the second card 2, along with its own serial number 23. The algorithm 21 for calculating the management code 22 of the second card receives, as inputs, the serial number 23 of the second card and data relating to the first card, such as its serial number 12 and/or its management code 14. The second management code 22 is generated in accordance with these inputs, and stored on the second card 2. (Page 6, line 23, to page 7, line 5).

VI. Grounds of Rejection to be Reviewed on Appeal

The final Office Action presents the following two grounds of rejection for review on this appeal:

1. Are claims 1-8 and 14-16 unpatentable under 35 U.S.C. §103, when the Ieki et al patent (U.S. 5,204,512) is considered in view of the Chen et al patent (U.S. 5,694,471) and the Bosen et al patent (U.S. 5,060,263)?

2. Are claims 9-13 and 17 unpatentable under 35 U.S.C. §103 when the Ieki, Chen and Bosen patents are considered in further view of the Drupsteen et al patent (U.S. 6,073,236)?

VII. Argument

Claims 1 and 14

Claim 1 recites a process to manage data stored in chip cards, in which a first management code is produced with a cryptographic algorithm based on a mother key and a first set of identification data of a first chip card, and is recorded in the memory of the first chip card. The editing of data stored in the memory is permitted if a secret code is presented that is compatible with the recorded first management code. The claim goes on to recite that a second management code is produced with a second cryptographic algorithm "based on data relating to the first card and a second set of identification data of a second chip card." The claim also recites that

"said data relating to the first card and the second management code are recorded in . . . the second chip card."

The rejections of the claims rely upon the Ieki patent as the principal reference. The Ieki patent is not directed to the same situation as the claimed subject matter, in which data from one card is transferred to another card. Rather, as discussed in the background portion of that patent, it is concerned with the need to regularly update the algorithm for enciphering data that is communicated between an IC card and a host computer. As described in the patent, the algorithm is typically stored in a ROM that is located in an intermediate communication device, e.g. a reader. When the algorithm is to be updated, the ROM containing the older algorithm must be replaced by a ROM storing the updated algorithm. This can result in a cumbersome procedure, particularly for the case in which the ROM is located in the communication device.

To alleviate the need for such a procedure, the Ieki patent discloses that the ROM can be provided in a separate IC card. In such a case, the communication device is provided with a first slot 13 to receive the principal IC card IC-2 that is used to communicate with a host computer HC, and a second slot 14 to receive another IC card IC-1 containing the encryption algorithm. Consequently, when the encryption algorithm is to be updated, it is only necessary to substitute a new card IC-1 containing the upgraded algorithm, rather than having to replace the ROM within the communication device 10.

Thus, while the Ieki patent discloses a system in which two IC cards are employed, it is not concerned with the particular type of operation to which the present invention is directed, namely the transfer of data from one card to the other. Rather, in the system of the Ieki patent, the two IC cards perform entirely different functions. The card IC-1 essentially functions as a component of the communication device 10, to implement the encryption algorithm. The principal IC card, IC-2, is employed in a standard manner for communication with the host computer HC.

As noted previously, claim 1 recites, among other elements, that data relating to the first card, as well as a second management code, are recorded in the second chip card. The Office Action asserts that the Ieki patent discloses this claimed

feature, with reference to column 4, lines 38-46 and 62-67. However, these portions of the patent do not disclose the claimed feature, nor do any other portions thereof.

First, it is to be noted that the rejection does not indicate which card in the Ieki patent is considered to correspond to the claimed first card and which one corresponds to the second card of claim 1. For purposes of discussion, it is assumed that the principal card for communication with the host computer, i.e., IC-2, is the first card. There is no disclosure in the Ieki patent that data relating to this card is stored in the other IC card. At best, at column 4, lines 62-67, the patent discloses that new data to be written in the first card IC-2 is enciphered in the host computer and provided to the second card IC-1 to be deciphered. The deciphered data is then stored in the first card IC-2.

This disclosure does not constitute a teaching of storing data relating to the first card in the second card. The data that is sent to the card IC-1 to be deciphered is not data that *relates* to the first card. For instance, claim 6 recites that the data relating to the first card comprises identification data for the first card. Claim 7 recites that the data relating to the first card comprises a first management code for the first card. The Ieki patent does not disclose that the data that is deciphered in the card IC-1 *relates* to the card IC-2 in such a fashion, namely that it serves to identify the card or to control its operation. The patent only refers to generic "data", without specifying its nature.

Another feature recited in claim 1 is that a second management code is produced on the basis of data relating to the first card and a set of identification data of the second card. It is "said" data relating to the first card that is stored in the second card. In other words, the data relating to the first card that is stored in the second card is also the data that is used to produce the second management code. There is no disclosure in the Ieki patent that any data passing through the card IC-1, to be deciphered and then subsequently stored in the card IC-2, is used to produce a management code for the card IC-1. The Ieki patent does not disclose how management codes are produced for the cards, particularly what data is used to generate them. Accordingly, even when the teachings of the Ieki patent are given

their broadest reasonable interpretation, they do not suggest the type of relationship that is recited in claim 1.

In addition to this claimed relationship, the combination of references does not disclose the concept of generating a second management code in accordance with data relating to a first chip card and identification data of a second chip card. This subject matter is recited in both claim 1 and claim 14. The rejection acknowledges that this claimed feature is not taught by the Ieki and Chen patents, even when considered in combination. Accordingly, it relies upon the Bosen patent, particularly at column 4, lines 27-49 and column 6, lines 58-67. However, the Bosen patent cannot be interpreted to disclose, nor otherwise suggest, the claimed subject matter. First, it is not concerned with systems that employ chip cards, let alone first and second chip cards. Rather, it discloses a system for dynamically generating a new password each time a user desires to access a computer. Unlike a static password system, in which the user enters the same password each time protected data is accessed, a dynamic password system requires the user to enter a different password for each access. The Bosen patent teaches that the new password is computed by encrypting the previous password in a number of steps. Column 7, lines 40-47. In this type of system, the new password replaces the previous password each time the protected data is accessed.

The Bosen patent is only concerned with access to a *single* device, or program. There is no teaching in this patent which would lead a person of ordinary skill in the art to generate a management code for a *second* device, such as a chip card, on the basis of data relating to a first device and identification data of the second device. Since the Bosen patent only relates to the operation of a single device, it cannot be interpreted to teach the generation of management codes that are based upon information relating to two different devices.

None of the three references teaches this concept. Consequently, any possible combination of their teachings cannot be deemed to suggest the claimed subject matter. At best, when the teachings of the *Bosen* patent are applied to the combined disclosures of the *Ieki* and *Chen* patents, the logical result would be to employ dynamic password protection in place of the static password protection, for a

given IC card. There is no suggestion, however, in any of the references that the password, or other access control code, for a *second* IC card should be based upon data relating to the first card. As noted above, the *Ieki* patent discloses that the password protection data of the two cards is independent of one another, and there is nothing in either the *Chen* or the *Bosen* patents that suggests modifying this teaching in a manner that would result in the claimed subject matter.

Second, the Office Action does not provide any motivation that would lead a person of ordinary skill in the art to combine the teachings of the Bosen patent with the systems of the Ieki and Chen patents. As noted above, the Bosen patent has nothing to do with chip card systems, let alone systems that employ two chip cards. Consequently, it is not apparent why a person of ordinary skill in the art would refer to the teachings of the Bosen patent, particularly if he were faced with the problem addressed by the present invention, namely the transfer of data from one chip card to another chip card. The issues addressed by the Bosen patent have nothing to do with this type of operation.

Claim 4

Claim 4 recites that the first cryptographic algorithm is different from the second cryptographic algorithm. These two algorithms are used to produce the first and second management codes, respectively. In rejecting this claim, the Office Action refers to the Ieki patent at column 2, lines 12-24. However, this portion of the patent does not relate to the algorithms for generating management codes. As noted previously, the Ieki patent does not disclose how the management codes are produced. Rather, as acknowledged in the Action, the patent is referring to cryptographic communication algorithms, i.e. for enciphering data that is communicated between two devices. This teaching has nothing to do with algorithms for producing management codes. It does not provide any suggestion that the algorithm for producing a code number for card IC-1 should be different from an algorithm for producing a code for card IC-2.

Claims 9-17

Claims 9-17 recite, among other features, storing an attribute in the first card in association with data stored therein, and using the attribute to determine whether to generate the second management code. In connection with this subject matter, the Office Action refers to the Drupsteen patent at column 5, lines 17-39. This portion of the patent relates to a flag register, illustrated in Figure 5. The flags in this register indicate whether individual application-specific commands are to be executed, to prevent unauthorized or inadvertent execution. This teaching has nothing to do with whether a management code is to be generated for a second chip card when copying data from one card to another. The rejection alleges that this claimed feature "would have been obvious," but provides no support in any of the references for such a conclusion. The rejection is based solely on hindsight knowledge of the invention.

VIII. Claims Appendix

See attached Claims Appendix for a copy of the claims involved in the appeal.

IX. Evidence Appendix

(None)

X. Related Proceedings Appendix

(None)

XI. Conclusion

For the reasons presented above, the references do not disclose all of the steps of the methods recited in the claims. The rejections are not properly founded in the statute, and should be reversed.

Respectfully submitted,

Buchanan Ingersoll PC

Date September 27, 2005 By: 

James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

VIII. CLAIMS APPENDIX

The Appealed Claims

1. Process to manage data stored in a first memory of a first chip of a first chip card in which:

a first management code is produced with a first cryptographic algorithm based on a mother key and a first set of identification data of the first chip card,

said first management code is recorded in the first memory,

the first card is linked to a chip card reader, and

editing of data stored in the first memory is authorized if a secret code presented to the reader is compatible with the recorded first management code,

wherein the following steps are performed:

a second management code is produced with a second cryptographic algorithm based on data relating to the first card and a second set of identification data of a second chip card,

said data relating to the first card and the second management code are recorded in a second memory of a second chip of the second chip card, and

editing of the data stored in the second memory is authorized if a secret code presented to the reader is compatible with the recorded second management code.

2. The process according to claim 1 wherein the first and second management codes are secret codes.

3. The process according to claim 1 wherein the second algorithm is implemented in the chip of the card.

4. The process according to claim 1 wherein the first cryptographic algorithm is different from the second cryptographic algorithm, and the second cryptographic algorithm is symmetric.

5. The process according to claim 1, wherein the first cryptographic algorithm is the same as the second cryptographic algorithm.

6. The process according to claim 1, wherein the data relating to the first card is the first set of identification data of the first card or the first chip.

7. The process according to claim 1, wherein the data relating to the first card is the first management code of the first card or the first chip.

8. The process according to claim 1 wherein a management code word is produced in the reader on the basis of the data relating to the first card, and a determination is made whether the card is authentic if said management code word is compatible with a secret word.

9. The process according to claim 1 wherein a transmission attribute is associated with the data stored in the first memory, editing of these data is authorized so that they can be copied into the second memory depending on the value of this attribute, these data and this attribute are copied into the second memory, and this attribute gives information about a need to produce a second secret code when copying the data.

10. The process according to claim 9 wherein, in order to authorize editing of data contained in the first memory only under the control of a master system, a transmission attribute which gives information about a need for said control by a master system is associated, this attribute is read prior to editing, and an editing program is started if the attribute having been read allows such_control.

11. The process according to claim 9 wherein the transmission attribute inhibits editing with a view to the data concerned being copied.

12. The process according to claim 9 wherein the data is copied into the memory in delayed time.

13. The process according to claim 1, wherein the card is a multi-application card, the data being associated with respective management codes.

14. A method for managing data stored in plural chip cards, comprising the following steps:

generating a first management code in accordance with a first cryptographic algorithm that is based upon an encryption key and identification data of a first chip card;

storing said first management code in said first chip card;

permitting access to data stored in said first chip card only if a code presented by a user is compatible with said first management code;

generating a second management code in accordance with a second cryptographic algorithm that is based upon data relating to said first chip card and identification data of a second chip card;

storing said second management code in said second chip card; and

permitting access to data stored in said second chip card only if a code presented by a user is compatible with said second management code.

15. The method of claim 14 wherein said data relating to said first chip card includes said identification data of said first chip card.

16. The method of claim 14 wherein said data relating to said first chip card includes said first management code.

17. The method of claim 14 further including the steps of:

storing an attribute in said first chip card in association with said data stored in said first chip card;

copying said data stored in said first chip card and said attribute to said second chip card;

detecting the value of said attribute; and

selectively generating said second management code and storing it in said second chip card in response to the detected value of said attribute.